BENDAU & BENDAU PLLC
Clifford P. Bendau, II (AZ Bar No. 030204)
Christopher J. Bendau (AZ Bar No. 032981)
P.O. Box 97066
Phoenix, Arizona 85060
Telephone: (480) 382-5176
Fax: (480) 304-3805
Email: cliffordbendau@bendaulaw.com
chris@bendaulaw.com

LYNCH CARPENTER, LLP
Gary F. Lynch (To apply *pro hac vice*)
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel.: (412) 322-9243
gary@lcllp.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

Brenda Moreno-Decerra, *individually and on behalf of all others similarly situated*, Plaintiff, v. Medical Management Resource Group, L.L.C. d/b/a American Vision Partners, Defendant.	Case No.: CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Brenda Moreno-Decerra ("Plaintiff") brings this Class Action Complaint, on behalf of herself and all others similarly situated, against Medical Management Resource Group, L.L.C. d/b/a American Vision Partners ("MMRG" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to herself, which are based on personal knowledge:

NATURE OF THE ACTION

1. Companies that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This

duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data and privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. MMRG is a healthcare business that provides its partner ophthalmology practices with management systems, infrastructure, and technology. Through Defendant's partner ophthalmology practices, MMRG serves patients across Arizona, New Mexico, California, and Texas.[1]

4. As a healthcare business associate, MMRG knowingly obtains, collects, and stores patient PII and PHI. In turn, Defendant has a duty to secure, maintain, protect, and safeguard the PII and PHI that it collects and stores against unauthorized access and disclosure through reasonable and adequate data security measures.

5. Despite MMRG's duty to safeguard patients' PII and PHI, Plaintiff's and other patients' PII and/or PHI was accessed and exfiltrated by a threat actor during a data breach of Defendant's computer network which MMRG detected on or about November 23, 2023 (the "Data Breach").[2]

6. Based on the public statements of MMRG to date, a wide variety of patient PII and PHI was implicated in the Data Breach, including, but not limited to: patient names, contact

[1] *American Vision Partners*, https://americanvisionpartners.com/ (last visited Feb. 29, 2024).

[2] *MMRG Notifies Patients of Cybersecurity Incident*, Businesswire (Feb. 6, 2024), https://www.businesswire.com/news/beverlyhillschamber/20240206060527/en.

information, dates of birth, medical information (including services received, clinical records, and medications), Social Security Numbers, and insurance information.[3]

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patient PII and/or PHI. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient PII and/or PHI; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to monitor and timely detect the Data Breach.

8. As a result of Defendant's failure to implement and follow basic data security procedures, Plaintiff's and Class Members' PII and PHI is now in the hands of cybercriminals who wish to use it for nefarious purposes.

9. As a result of MMRG's inadequate data security and a breach of its duties and obligations, Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, intrusion on their health privacy, and similar forms of criminal mischief, risks which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

10. Plaintiff, on behalf of herself and all others similarly situated, alleges claims for negligence, negligence *per se*, unjust enrichment, and declaratory judgment, and seeks to compel Defendant to adopt reasonably sufficient security practices to safeguard patient PII and PHI that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future and to further provide Plaintiff and Class Members with credit monitoring services for the rest of their lives.

[3] *Id.*

11. To recover from Defendant for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendant to: (1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; (2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Defendant; and (3) provide, at its own expense, all impacted victims with lifetime identity protection services.

PARTIES

12. Plaintiff is and was, at all relevant times hereto, an adult who is a resident of the State of Arizona. Plaintiff received a notification from Defendant indicating that her PII and/or PHI in MMRG's possession had been compromised in the Data Breach.

13. Defendant MMRG is an Arizona limited liability company with its headquarters located in Tempe, Arizona. Upon information and belief, Defendant is owned by two members: American Vision Partners Corporation and American Vision Partners Holding Corporation. American Vision Partners Corporation is a Delaware corporation with a principal place of business located in Tempte, Arizona. American Vision Partners Holding Corporation is a Delaware corporation with a principal place of business located in Tempte, Arizona.

14. Defendant MMRG is a citizen of each State in which one of its members is a citizen. Defendant MMRG is therefore a citizen of the States of Delaware and Arizona.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2)(A), because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

16. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District, and Defendant resides in this District.

17. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL BACKGROUND

A. MMRG Collected and Stored Plaintiff's and Class Members' PII & PHI.

18. MMRG operates as an eye care management organization and active ophthalmology practice consolidator. Defendant has partnered with and operates numerous eye care centers and ambulatory surgical centers across Arizona, New Mexico, California, and Texas.

19. Defendant and its partner ophthalmology practices operate as one eye care practice, as MMRG assists its partners with: referral management, surgery centers, marketing and branding, physician relations, centralized scheduling, facilities management, purchasing and inventory management, optical support, regulatory compliance, contract review, market analysis, call centers, payor analysis, contract negotiation, payroll, benefit management, employee relations support, recruiting, training and staffing, day to day management, contracting and credentialing, billing and collections, revenue recognition, accounting and finance, forecasting, and budgeting.[4]

20. In the regular course of its business, MMRG collects and maintains the PII and PHI of current and former patients of its partner ophthalmology practices. This information includes patient names, contact information, dates of birth, medical information (including services received, clinical records, and medications), Social Security Numbers, and insurance information.

21. In order to receive healthcare services from Defendant's ophthalmology partners, MMRG required Plaintiff and Class Members to entrust Defendant with their sensitive and confidential PII and PHI, and Plaintiff and Class Members therefore reasonably expected that Defendant would safeguard their highly sensitive PII and keep their PHI confidential.

22. Due to the sensitivity of the PII and PHI that MMRG collects, stores, and handles, it is aware of its critical responsibility to safeguard this information—and how devastating its theft is to individuals whose information has been stolen.

[4] *Solutions*, American Vision Partners, https://americanvisionpartners.com/partnerships/solutions/ (last visited Feb. 29, 2024).

23. By obtaining, collecting, and storing Plaintiff's and Class Members' PII and PHI, MMRG assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

24. Despite the existence of these duties, MMRG failed to implement reasonable data security measures to protect Plaintiff's and Class Members' PII and PHI, and ultimately allowed nefarious third-party hackers to access and exfiltrate Plaintiff's and Class Members' PII and PHI.

B. MMRG Is a "Business Associate" That Must Comply with HIPAA.

25. MMRG is a Health Insurance Portability and Accountability Act ("HIPAA")-covered business associate that provides services to various healthcare providers (referred to by HIPAA as "Covered Entities"). As a regular and necessary part of its business, MMRG collects and custodies the highly sensitive PHI of its ophthalmology partner's patients. MMRG is required under federal law to maintain the strictest confidentiality of the patients' PHI that it acquires, receives, and collects, and MMRG is further required to maintain sufficient safeguards to protect that PHI from being accessed by unauthorized third parties.

26. As a HIPAA-covered business associate, MMRG is required to enter into contracts with its Covered Entities to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of PHI, including by implementing requirements of the HIPAA Security Rule and to report to the Covered Entities any unauthorized use or disclosure of PHI, including incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

27. As a condition of receiving MMRG's services, Defendant requires that Covered Entities and their patients, including Plaintiff and Class Members, entrust it with highly sensitive personal information. Due to the nature of MMRG business, which includes practice management solutions for its ophthalmology partners, Defendant would be unable to engage in its regular business activities without collecting and aggregating PHI that it knows and understands to be sensitive and confidential.

28. Plaintiff and Class members are or were patients whose PHI was maintained by or who received health-related services though MMRG through its ophthalmology partners, and directly or indirectly entrusted MMRG with their PHI. Plaintiff and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

C. MMRG Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims.

29. MMRG was well aware that the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

30. MMRG also knew that a breach of its computer networks, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

31. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and other healthcare partner and provider companies, including Managed Care of North America, OneTouchPoint, Inc., Shields Healthcare Group, Eye Care Leaders, Connexin Software, Inc., and Blackbaud.

32. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[5] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

33. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches,

[5] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last accessed Dec. 11, 2023).

exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[6]

34. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[7]

35. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[8] Indeed, "[t]he IT environments of healthcare organizations are often complex and difficult to secure. Devices and software continue to be used that have reached end-of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that have been developed to work on specific – and now obsolete – operating systems and cannot be transferred to supported operating systems."[9]

36. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure of the information of 382,262,109 individuals—"[t]hat equates to more than 1.2x the population of the United States."[10]

---

[6] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/ (last accessed Dec. 11, 2023).

[7] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last accessed Dec. 11, 2023).

[8] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Dec. 11, 2023).

[9] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA Journal (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in%20victims'%20names (last accessed Dec, 11, 2023).

[10] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last accessed Dec. 11, 2023).

37. Further, the rate of healthcare data breaches has been on the rise in recent years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[11]

38. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[12]

39. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[13]

40. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves MMRG's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

41. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Social Security Numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

42. The Social Security Administration even warns that the process of replacing a Social Security Number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

---

[11] *Id.*

[12] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last accessed Dec. 11, 2023).

[13] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last accessed Dec. 11, 2023).

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[14]

43. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often Social Security Numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

44. **Medical Information**—As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[15] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[16]

---

[14] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Dec. 11, 2023).

[15] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, *New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last accessed Dec. 11, 2023).

[16] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last accessed Dec. 11, 2023).

45. Indeed, medical records "are so valuable because they can be used to commit a multitude of crimes. Healthcare data can be used to impersonate patients to obtain expensive medical services, Medicare and Medicaid benefits, healthcare devices, and prescription medications. Healthcare records also contain the necessary information to allow fraudulent tax returns to be filed to obtain rebates."[17]

46. "In contrast to credit card numbers and other financial information, healthcare data has an incredibly long lifespan and can often be misused for long periods undetected. Credit card companies monitor for fraud and rapidly block cards and accounts if suspicious activity is detected, but misuse of healthcare data is harder to identify and can be misused in many ways before any malicious activity is detected. During that time, criminals can run up huge debts – far more than is usually possible with stolen credit card information."[18]

47. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage, or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[19]

48. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before

---

[17] Alder, *supra* note 14.

[18] *Id.*

[19] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed Dec. 11, 2023).

being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[20]

49. **Health Insurance Information**—"stolen personal health insurance information can be used by criminals to obtain expensive medical services, devices and prescription medications, as well as to fraudulently acquire government benefits like Medicare or Medicaid."[21]

50. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

51. Based on the value of the PII and PHI of its ophthalmology partners' patients to cybercriminals, MMRG knew or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. MMRG failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

[20] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last accessed Dec. 11, 2023).

[21] Kate O'Flaherty, *Why cyber-Criminals Are Attacking Healthcare -- And How to Stop Them*, Forbes (Oct. 5, 2018), https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/?sh=54e8ed1e7f69 (last accessed Dec. 11, 2023).

D. MMRG Breached its Duty to Protect Patients' PII and PHI.

52. On or about February 6, 2024, Defenant announced that it had suffered a cybersecurity incident and was in the process of notifying individuals impacted by the Data Breach.[22]

53. According to MMRG, on or about November 14, 2023, Defendant detected unauthorized activity on its computer network. Following discovery of the intrusion, MMRG began an investigation into the data breach.[23]

54. Following the investigation, on or about December 6, 2023, MMRG concluded that during the Data Breach an unauthorized party gained access to and stole the personal information associated with patients of Defendant's ophthalmology partners.[24] The patient information exfiltrated includes: patient names, contact information, dates of birth, medical information (including services received, clinical records, and medications), Social Security Numbers, and insurance information.[25]

55. Based on MMRG's announcement, it is unclear when the Data Breach began, how long the Data Breach occurred, when MMRG took action to stop the Data Breach, and whether the Data Breach has actually been stopped.

56. It is evident that the unauthorized actor accessed MMRG's computer network in an attack designed to acquire sensitive, confidential, and valuable PII and PHI stored therein, and that they were successful in the attack. Based on Defendant's disclosures, the PII and PHI stolen by cybercriminals was not encrypted.

57. On or about February 6, 2024, MMRG reported the Data Breach to United States Department of Health and Human Services Office for Civil Rights ("HHS"), indicating that the

[22] *MMRG Notifies Patients of Cybersecurity Incident*, *supra* note 2.
[23] *Id.*
[24] *Id.*
[25] *Id.*

Data Breach impacted approximately 2.3 million individuals.[26] Over a week later, on or about February 15, 2024, Defendant began notifying impacted patients of the Data Breach.[27]

58. On Plaintiff's information and belief, the Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures in order to protect the PII and PHI of its partner ophthalmology practices' patients.

E. MMRG Failed to Comply with FTC Guidelines and Industry Best Practices.

59. MMRG is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act

60. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[28]

61. In 2016, the FTC updated its publication titled Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.[29] The guidelines state that:

a. businesses should promptly dispose of personal identifiable information that is no longer needed, and retain sensitive data "only as long as you have a business reason to have it;"

[26] *Cases Currently Under Investigation*, US DHHS OCR, available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Feb. 29, 2024).

[27] *Data Breach Notifications*, *Office of the Maine Attorney General*, https://apps.web.maine.gov/online/aeviewer/ME/40/1c20fc77-1b3a-44a9-81e0-362f8bed0912.shtml (last visited Mar. 1, 2024).

[28] *Start with Security: A Guide for Business*, Fed. Trade Comm'n, https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last accessed Dec. 11, 2023).

[29] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission, October 2016, available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Dec. 11, 2023).

b. businesses should encrypt sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c. businesses should thoroughly understand the types of vulnerabilities on their network and how to address those vulnerabilities;

d. businesses should install intrusion detection systems to promptly expose security breaches when they occur; and

e. businesses should install monitoring mechanisms to watch for large troves of data being transmitted from their systems.

62. In another publication, the FTC recommended that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[30]

63. Notably, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the FTC Act. Indeed, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

64. MMRG was at all times fully aware of its obligations to protect the PII and PHI of its partner ophthalmology practices' patients because of its position as a business associate of covered entities, which gave it access to reams of patient PII and PHI. MMRG was also aware of the significant repercussions that would result from its failure to do so.

[30] *See Start with Security: A Guide for Business*, Federal Trade Commission, June 2015, available at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business. (last accessed Dec. 11, 2023).

65. Upon information and belief, MMRG failed to properly implement one or more of the basic data security practices recommended by the FTC. MMRG failure to employ reasonable and appropriate data security measures to protect against unauthorized access to patients' PII and/or PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

66. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[31]

67. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[32] Upon information and belief, MMRG failed to adhere to the NIST guidance.

68. Further, cybersecurity experts have identified various best practices that should be implemented by entities in the healthcare security, including implementing the following measures:

a. Email protection systems and controls;

b. Endpoint protection systems;

c. Identify all users and audit their access to data, application, systems, and endpoints;

d. Data protection and loss prevention measures;

e. IT asset management;

f. Network management;

g. Vulnerability management;

h. Security operations center & incident response; and

[31] *See Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, available at https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (last accessed Dec. 11, 2023).

[32] *Id.* at Table 2 pg. 26-43.

i. Cybersecurity oversight and governance policies, procedures, and processes.[33]

69. Upon information and belief, Defendant's failure to protect massive amounts of PII is a result of its failure to adopt reasonable safeguards as required by the FTC guidelines, NIST guidance, and industry best practices.

70. MMRG was well aware of its obligations to use reasonable measures to protect patients' PII and PHI. MMRG also knew it was a target for hackers, as discussed above. Despite understanding the risks and consequences of inadequate data security, Defendant nevertheless failed to comply with its data security obligations.

F. MMRG is Obligated Under HIPAA to Safeguard Patient PHI.

71. MMRG is required by HIPAA, 42 U.S.C. § 1302d, *et seq*. to safeguard patient PHI.

72. As a business associate of healthcare providers, MMRG is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

73. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

74. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

75. Under 45 C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either "(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

[33] *HICP's 10 Mitigating Practices*, HHS, https://405d.hhs.gov/best-practices (last accessed Dec. 11, 2023).

76. HIPAA requires MMRG to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et seq*.

77. HHS further recommends the following data security measures a regulated entity such as MMRG should implement to protect against some of the more common, and often successful, cyber-attack techniques:

a. regulated entities should implement security awareness and training for all workforce members and that the training programs should be ongoing, and evolving to be flexible to educate the workforce on new and current cybersecurity treats and how to respond;

b. regulated entities should implement technologies that examine and verify that received emails do not originate from known malicious site, scan web links or attachments included in emails for potential threats, and impeded or deny the introduction of malware that may attempt to access PHI;

c. regulated entities should mitigate known data security vulnerabilities by patching or upgrading vulnerable technology infrastructure, by upgrading or replacing obsolete and/or unsupported applications and devices, or by implementing safeguards to mitigate known vulnerabilities until an upgrade or replacement can occur;

d. regulated entities should implement security management processes to prevent, detect, contain, and correct security violations, including conducting risk assessments to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI; and

e. regulated entities should implement strong cyber security practices by requiring strong passwords rules and multifactor identification.[34]

78. Upon information and belief, MMRG failed to implement one or more of the recommended data security measures.

79. While HIPAA permits healthcare providers and their business associates to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals, nor did Plaintiff or the Class Members consent to the disclosure of their PHI to cybercriminals.

80. As such, Defendant is required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that it acquires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

81. Given the application of HIPAA to MMRG, and that Plaintiff and Class Members directly or indirectly entrusted their PHI to Defendant in order to receive healthcare services from MMRG's partner ophthalmology practices, Plaintiff and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

G. Plaintiff and Class Members Suffered Damages.

82. For the reasons mentioned above, MMRG's conduct, which allowed the Data Breach to occur, caused Plaintiff and members of the Class significant injuries and harm in several ways. Plaintiff and members of the Class must immediately devote time, energy, and money to: (1) closely monitor their medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing

[34] *OCR Quarter 1 2022 Cybersecurity Newsletter*, U.S. Dept't of Health & Human Services (Mar. 17, 2023), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html (last accessed Dec. 11, 2023).

attack; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

83. Once PII and PHI are exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct. Further, the value of Plaintiff's and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

84. As a result of MMRG's failures, Plaintiff and Class Members are at substantial and increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

85. With respect to healthcare breaches, a study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[35]

86. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[36]

87. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[37]

88. Health information in particular is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[38]

[35] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HealthITSecurity, https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud (last visited Jan. 9, 2024).

[36] *Id.*

[37] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

[38] *Id.*

89. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[39]

90. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect the PII and PHI of its partner ophthalmology practices' patients.

91. Furthermore, Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to unauthorized third parties.

Plaintiff's Experience.

92. Plaintiff is a patient of one of MMRG's partner ophthalmology practices. In order to receive healthcare services from MMRG's partner ophthalmology practice, plaintiff was required to provide and entrust her PII and PHI to Defendant. In requesting and maintaining Plaintiff's PII and PHI, MMRG undertook a duty to act reasonably in its handling of Plaintiff's PII and PHI. MMRG, however, did not take reasonable care of Plaintiff's PII and PHI, leading to its unauthorized access and exfiltration as a result of Defendant's inadequate data security measures.

93. Plaintiff received a Notice dated February 15, 2024 from MMRG informing her that her PII and PHI provided to Defendant was compromised in the Data Breach. The Noice put the onus on Plaintiff to protect her PII and PHI by encouraging Plaintiff to remain vigilant and recommending that she regularly review her account statements and credit reports and report any suspicious or unrecognized activity immediately.

[39] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, Experian, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Jan. 9, 2024).

94. Since the Data Breach, Plaintiff has noticed a marked increase in spam texts and emails asking her to respond. Plaintiff noticed that this was a substantial increase to the amount of spam texts and emails that she received prior to the Data Breach.

95. Since the Data breach, Plaintiff has also been required to spend her valuable time and effort to mitigate her risk of identity theft and fraud, including spending time researching the Data Breach.

96. Plaintiff has suffered actual injury from having her PII and PHI exposed and/or stolen as a result of the Data Breach, including: (1) required mitigation efforts, including needing to monitor her financial and medical accounts to ensure her information is not used for identity theft and fraud; (b) damages to and diminution of the value of her PII and PHI, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; and (c) loss of privacy.

97. In addition, knowing that hackers accessed and likely exfiltrated her PII and PHI and this information likely has been and will be used in the future for identity theft, fraud, and other nefarious purposes has caused Plaintiff to experience significant frustration, anxiety, worry, stress, and fear.

98. As a direct and proximate result of the Data Breach, Plaintiff has been and will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending and is not speculative given the highly sensitive nature of the PII and PHI compromised in the Data Breach.

CLASS ACTION ALLEGATIONS

99. Plaintiff brings this class action on behalf of herself and all others who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

100. Plaintiff seeks to represent the following Class of persons defined as follows:

> All individuals in the United States whose PII and/or PHI was compromised in the MMRG Data Breach which was announced on or about February 6, 2024 (the "Class").

101. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

102. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

103. **Numerosity:** The members of the Class are so numerous that the joinder of all members is impractical. Plaintiff is informed and believes, and thereon alleges, that there are millions of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through MMRG's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 2.3 million individuals.

104. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether MMRG had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether MMRG was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of MMRG's wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of MMRG's wrongful conduct.

105. **Typicality:** Plaintiff's claims are typical of the claims of Class Members. Plaintiff's and Class Members' claims are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and Class Members each had their PII and PHI exposed and/or accessed by an unauthorized third party.

106. **Adequacy:** Plaintiff is an adequate representative of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the Class Members and has no interests antagonistic to the Class Members. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

107. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all Class members is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

108. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

109. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that generally apply to the Class making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

110. **Ascertainability:** Class Members are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through MMRG's books and records.

FIRST CAUSE OF ACTION

UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

111. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

112. MMRG owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

113. MMRG's duty to use reasonable care arose from several sources, including but not limited to those described below.

114. MMRG had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By receiving, maintaining, and handling PII and PHI that are routinely targeted by criminals for unauthorized access, MMRG was obligated to act with reasonable care to protect against these foreseeable threats. Furthermore, MMRG knew or should have known that, if hackers accessed the sensitive data contained in its data systems, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and the Class, was the foreseeable consequence of Defendant's unsecured, unreasonable data security measures.

115. MMRG's duty also arose from its position as a business associate of covered entities. MMRG holds itself out as a trusted provider of healthcare management services, thereby assuming a duty to reasonably protect the information it obtains from its partner ophthalmology practices' patients. Indeed, MMRG, which receives, maintains, and handles PII and PHI from its partners' patients, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

116. MMRG also owed a common law duty because its conduct created a foreseeable risk of harm to Plaintiff and Class Members. MMRG's conduct included its failure to adequately restrict access to its computer networks that held patient PII and PHI.

117. MMRG also knew or should have known of the inherent risk in collecting and storing massive amounts of PII and PHI, the importance of implementing adequate data security measures to protect that PII and PHI, and the frequency of cyberattacks such as the Data Breach in the healthcare sector.

118. MMRG breached the duties owed to Plaintiff and Class Members and thus was negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, MMRG breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its clients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

119. But for MMRG's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

120. As a direct and proximate result of MMRG's negligence, Plaintiff and Class Members have suffered injuries, including: (a) actual identity theft; (b) the loss of the opportunity how their PII and/or PHI is used; (c) the compromise, publication, and/or theft of their PII and/or PHI; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from

identity theft, and/or unauthorized use of their PII and/or PHI; (e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII and/or PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and/or PHI in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and/or PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

121. As a direct and proximate result of MMRG's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

/ / /

/ / /

SECOND CAUSE OF ACTION

NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

122. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

123. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities, such as MMRG, for failing to use reasonable measures to protect individuals' PII and PHI. Various FTC publications and orders also form the basis of Defendant's duty.

124. MMRG violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored from

its partner ophthalmology practices' patients and the foreseeable consequences of a data breach involving member PII and PHI.

125. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

126. The harm that has occurred as a result of MMRG's conduct is the type of harm that the FTC Act was intended to guard against.

127. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

128. MMRG is an entity covered under the HIPAA, which sets minimum federal standards for privacy and security of PHI.

129. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., and its implementing regulations, MMRG had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class Members' electronic PHI.

130. Specifically, HIPAA required MMRG to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, et. seq.

131. HIPAA also requires MMRG to provide Plaintiff and Class Members with notice of any breach of their individually identifiable PHI "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach." 45 C.F.R. §§ 164.400-414.

132. MMRG violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI; and by failing to provide Plaintiff and Class Members with notification of the Data Breach within 60 days after its discovery.

133. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect, as they are patients of MMRG's partner ophthalmology practices.

134. The harm that has occurred as a result of MMRG's conduct is the type of harm that HIPAA was intended to guard against.

135. MMRG's violation of HIPAA constitutes negligence per se.

136. As a direct and proximate result of MMRG's negligence, Plaintiff and Class Members have suffered injuries, including those identified in paragraph 136 above.

137. As a direct and proximate result of MMRG's negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION

UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

138. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

139. Plaintiff brings this claim individually and on behalf of the Class.

140. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PHI that was conveyed to, collected by, and maintained by MMRG and that was ultimately compromised and/or exfiltrated during the Data Breach.

141. Plaintiff and Class Members conferred a monetary benefit upon MMRG in the form of monies paid for healthcare services or other services. MMRG's business model would not exist save for the need to ensure the security of Plaintiff's and Class Members' PII and PHI in order to provide practice management solutions to its partner ophthalmology practices.

142. The relationship between MMRG is not attenuated, as Plaintiff and Class Members had a reasonable expectation that the security of their PII and PHI would be maintained when they provided their information to MMRG's partner ophthalmology practices. Indeed, MMRG boasts that it operates with its partner ophthalmology practices as one eye care practice.

143. MMRG accepted and/or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Upon information and belief, this financial benefit was, in, part conferred when Plaintiff and Class Members paid MMRG's partner ophthalmology practices for healthcare

services. Upon information and belief part of the monies Plaintiff and Class Members paid to their healthcare providers were shared with MMRG as part of the providers' relationships with MMRG. Defendant also benefited from the receipt of Plaintiff's and Class Members' PII and PHI.

144. MMRG also understood and appreciated that the PII and PHI pertaining to Plaintiff and Class Members was private and confidential and its value depended on MMRG maintaining the privacy and confidentiality of that information.

145. In particular, MMRG enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of MMRG's decision to prioritize its own profits over the requisite security.

146. MMRG failed to secure Plaintiff's and Class Members' PII and PHI and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

147. Defendant acquired the PII and PHI of Plaintiff and Class Members through inequitable means in that MMRG failed to disclose the inadequate security practices alleged above.

148. Under the principles of equity and good conscience, MMRG should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement appropriate data management and data security measures.

149. But for MMRG's willingness to commit to properly and safely collecting, maintaining, and storing PII and PHI, such information would not have been transferred to and entrusted to MMRG. Further, if Defendant had disclosed that its data security measures were inadequate, MMRG would not have gained the trust of its partner ophthalmology practices and their patients.

150. MMRG's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the collection, maintenance, and inadequate security

of Plaintiff's and Class Members' PII and PHI, while at the same time failing to securely maintain that information from unauthorized access and compromise.

151. The benefit conferred upon, received, and enjoyed by MMRG was not conferred gratuitously, and it would be inequitable and unjust for MMRG to retain the benefit under the circumstances.

152. Plaintiff and Class Members have no adequate remedy at law.

153. As a direct and proximate result of MMRG's wrongful conduct, Plaintiff and Class Members have sustained injuries, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity how their PII and/or PHI is used; (c) the compromise, publication, and/or theft of their PII and/or PHI; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and/or PHI; (e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII and/or PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and/or PHI in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and/or PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

154. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services, or Defendant should be compelled to place a percentage of all future profits into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, designed to represent the value obtained by the use of the inadequately secured PII and/or PHI compromised as a result of the Data Breach.

FOURTH CAUSE OF ACTION

DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

155. Plaintiff restates and realleges all preceding allegations set forth above as if fully alleged herein.

156. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et. seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Class Action Complaint.

157. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether MMRG is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and PHI and remains at imminent risk that further compromises of her PII and/or PHI will occur in the future.

158. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that, among other things:

a. MMRG owed a legal duty to secure patients' PII and PHI under the common law, Section 5 of the FTC Act, and HIPAA; and

b. MMRG breached and continues to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

159. This Court also should issue corresponding prospective injunctive relief requiring MMRG to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and Class Members' PII and PHI.

160. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at MMRG. The risk

of another such breach is real, immediate, and substantial. If another breach at MMRG occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

161. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to MMRG if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to MMRG of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and MMRG has a pre-existing legal obligation to employ such measures.

162. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at MMRG, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and patients whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for relief as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For damages in an amount to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and

H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: March 5, 2024

By: **BENDAU & BENDAU PLLC**

/s/ Clifford P. Bendau, II
Clifford P. Bendau, II
Christopher J. Bendau

LYNCH CARPENTER, LLP
Gary F. Lynch (To apply *pro hac vice*)
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel.: (412) 322-9243
gary@lcllp.com

Attorneys for Plaintiff